# Information Operations for Canada

**By**

**Colonel J.D.R. Bourque**

**Seminar 8, Advanced Militaries Studies Course 1**

**6 November 1998**

**Information Operations for Canada**

*"Information is the key to successful military operations; strategically, operationally, and technically. From war to OOTW, the adversary who wins the Information War prevails"*

*General (Ret) Glenn Otis, 1991*

**Introduction**

It has been generally accepted that operations which control, manipulate, and exploit information are a legitimate component of modern warfare, as they support mission objectives. Indeed, information operations are seen not only as force multipliers, but powerful weapons in their own right. The importance of the conduct ofatioi08.83997 TtioOmporul weaponsit rm

In OOTW conducted within Canada and under the UN umbrella, Canada is likely to need some independent capacity. In peace support operations conducted as part of the NATO Alliance or a coalition of the willing and able, Canada will have to contribute to the extent that it can complement the capacity of its allies. The issue then becomes, how much and what type of capacity does Canada need?

**Aim**

This paper will determine the extent to which Canada's capacity to conduct information operations should be developed, focusing on resources, structures and the necessary political support. The paper will examine the full spectrum of information operations with particular emphasis on the demands of OOTW.

**Information Operations**

The importance of using information effectively during military operations was covered by Sun Tzu over 2,000 years ago. He wrote: "Thus the reason the farsighted ruler and his superior commander conquer the enemy at every move, and achieve successes far beyond the reach of the common crowd, is foreknowledge. Such foreknowledge cannot be had from ghosts and spirits, deduced by comparison with past events, or verified by astrological calculations. It must come from people – people who know the enemy's situation."[1]

[1] Roger T. Ames, *The Art of War* (US: Ballantine Books, 1993), p 91.

The situation has changed drastically in the past 2,000 years, but more particularly in the past 75 years with the technical evolution in communication and electronic systems. Although the basic premise that intelligence is paramount to military operations remains true, it has certainly moved beyond the human dimension. It is no longer necessary to be in close touch with an adversary to collect intelligence about his status or his operations. It can now be done with ghosts, systems that are far out of sight and out of reach.

**Doctrine and Definitions**

In order to recognise the importance of IO for the CF's future involvement in an OOTW environment, it is necessary to understand the current CF IO doctrine, some definitions, and its implication vis-à-vis the resources, the structures, and the political support. The recently published CF Information Operations (CF IO) document was issued under the direction of the 1997 Defence Planning Guidance. The CF IO doctrine recognises that IO is not only restricted to conflict and war but is applicable across the range of military operations including OOTW. The doctrine also acknowledges that IO must be integrated in a Government-wide strategy, in support of political and military objectives. Its doctrinal basis for the CF involvement in combined, joint, and interdepartmental or interagency operations extends to the co-ordination, co-operation, deconfliction,[2] participation and support, by other Canadian departments and agencies, industries, allies, and Non-Governmental Organisations (NGOs).

[2] Deconfliction is required to ensure that no other agencies or organisations are planning to conduct similar activities that could result in either duplication of effort or failures.

IO are conducted within the Global Information Infrastructure (GII). The GII is comprised of all individuals and equipment capable of receiving, processing or transmitting information.[3] The GII contains the Canadian National Information Infrastructure (NII) and the Defence Information Infrastructure (DII). The GII equipment includes all computer and display systems, all sensors, and all communication and connection nodes including satellites. The equipment, or information systems (INFOSYS), also includes all weapons systems that utilise these technologies. Information is defined as that which informs or has the potential to inform, and is a combination of content and meaning represented by symbols and media or conduit, used or useable in a particular context; information can be used or shared by the operations and the intelligence communities.[4]

The NII is defined as the Canadian content or owned segment of the GII. The DII is the shared or interconnected system of computers, communications, data, applications, security, people, training and other support structures serving DND local, national and world-wide information needs.[5] Although it is perceived that the DII is a component of the NII, in the context of intelligence gathering, it has boundaries that can extend to the GII. Hence, the CF IO are not bounded to the limits of the DII and it must be capable of exploiting the entire GII.

---

[3] Department of National Defence, B-GG-005-004/AF-033 *CF Information Operations* (Ottawa: DND Canada, 1998), ch 1, p 8.

[4] Ibid, p 8.

[5] Ibid, p 13.

The doctrine defines IO as actions taken in support of political and military objectives which influence decision makers by affecting other's information while exploiting and protecting one's own information.[6] IO is further sub-divided into offensive and defensive IO. Offensive IO includes actions taken to influence actual or potential adversarial decision-makers. It includes using Psychological Operations (PSYOP), deception, electronic warfare, intelligence, computer network attack, physical destruction, and special information operations.

Defensive IO includes actions taken to ensure that friendly decision-makers have timely access to necessary, relevant and accurate information and that they are protected from any adversary offensive IO efforts. It is defined as a process that integrates and co-ordinates policies, procedures, operations, intelligence, law and technology.[7]

Command and Control Warfare (C2W) can be both offensive and defensive. C2W is the integrated use of the military IO capabilities and includes operations security, deception, PSYOP, electronic warfare, and physical destruction. Defined as an application of IO in any military operations, it is considered a subset of IO and is aimed at either attacking or defending a set of Command and Control (C2) target sets, hence it is sub-divided in C2-Attack and C2-Protect. C2 target sets can include leadership assets, military infrastructure, civil infrastructure and weapons systems. C2-Attack prevents an effective C2 of adversary forces by denying information to, influencing, degrading, or destroying the adversary C2

[6] Department of National Defence, B-GG-005-004/AF-033 *CF Information Operations* (Ottawa: DND Canada, 1998), ch 1, p 2.

systems.[8] C2-Protect maintains effective C2 of own forces by turning to friendly advantage or negating adversary efforts to deny information to, influence, degrade, or destroy the friendly C2 systems.[9]

Another two critical elements of IO that will be discussed in this paper, are Public Affairs (PA) and Civil Affairs (CA). Close co-ordination will ensure that the PA initiatives support the commander's overall objectives, and provide a timely flow of information to both external and internal audiences.[10] PA activities can influence an adversary's perception about the friendly force's intent, capability and vulnerability[11] and can be activated during any phase of a mission. It can be used to inform internal and external audiences of significant developments and encourage a favourable attitude toward the mission.[12] As well, CA are important to IO and must also be co-ordinated because of their ability to interface with key organisations and assist the commander's IO objectives by co-ordinating with, influencing, developing, or controlling indigenous infrastructures in foreign operational uses.[13] CA activities include Civil Military Co-operation (CIMIC)[14] which could be extended to the requirement to negotiate and mediate with belligerents.[15]

---

[7] Ibid, ch 3, p 8.

[8] Ibid, ch 3, p 15.

[9] Ibid, ch 3, p 15.

[10] Ibid, ch 2, p 15.

[11] Ibid, ch 2, p 7.

[12] Ibid, ch 2, p 7.

[13] Ibid, ch 2, p 15.

[14] CIMIC is defined as those activities that establish, maintain, influence and improve relations among military forces, civil authorities, and the civilian populace to facilitate military operations.

It is necessary to link the overall IO structure with INFOSYS and intelligence support, as both provide the cornerstone for offensive and defensive IO. INFOSYS are the stem of IO, as without them, nothing in the realm of the information world would exist, not even intelligence.[16] On the other hand, intelligence is also paramount to IO and in his book, Roger T. Ames introduces intelligence as: "… is of the essence in warfare – it is what the armies depend upon in their every move."[17] In the CF IO, intelligence is defined as the product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas; also, information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding.[18] Intelligence support is critical to the planning, execution, and assessment of IO; it must support the intelligence preparation of the battle-space[19] by identifying adversary threats and providing offensive or defensive measures against them.[20]

---

Department of National Defence, B-GL-300-001/FP-000 *Conduct of Land Operations - Operational Level Doctrine for the Canadian Army* (Ottawa: DND Canada, 1998), ch 7, p 11.

[15] Ibid, ch 2, p 8.

[16] INFOSYS collect, transport, process, disseminate, and display information used to support offensive and defensive IO.
Ibid, ch 3, p 11.

[17] Roger T. Ames, *The Art of War* (US: Ballantine Books, 1993), p 171.

[18] Department of the Army, FM 100-6 *Information Operations Doctrine*, (Washington, DC: Government Printing Office,1996), Gossary-8.

[19] The Intelligence Preparation of the Battle-space (IPB) is the continuous process used to develop and maintain a detailed knowledge of the adversary's use of information and information systems.
Department of National Defence, B-GG-005-004/AF-033 *CF Information Operations* (Ottawa: DND Canada, 1998),ch 2, p 16.

[20] Ibid, ch 2, pp 15-16.

This brief overview of the CF IO doctrine and definitions illustrates that the CF foresee the full spectrum of IO activities as applicable to the conduct of future military operations and OOTW, whether at home or abroad. Moreover, the doctrine is designed to be all encompassing and compatible with the NATO doctrine. What is of concern however, is to whether or not the CF IO doctrine is affordable. It is vital to be able to communicate with other nations and recognise the importance of IO, but it is also crucial to understand that without IO resources, the CF may no longer be able to operate effectively, in any missions. The point has to be made that IO may not only affect the CF whether at home or abroad, but that IO has the potential, through the interconnectivity of INFOSYS, to affect the entire nation. Through communication networks, an INFOSYS acquiring an undetected virus in an Area of Operation (AO)[21] may implant this virus to several INFOSYS of a nation. Canada must in turn understand that IO represent a new requirement and that it may require extra funding. If the CF try to develop this capability under their current funding envelope, they may further reduce their current overall capabilities for the sake of providing at best, a mediocre IO capability. Political support for extra funding may have to be sought if Canada wishes its military to be successful in future operations.

**OOTW**

[21] An Area of Operation (AO) can be defined as geographical areas in which operations are conducted. AOs used to be very concentrated in the distant past, hence easily manageable. Throughout centuries of conflicts, these limited and well-defined AOs have increased extensively and eventually became barely manageable (WW1, WW2). Yet, in the past few years, because of the information evolution, AOs have increased exponentially, to the point where boundaries are no longer geographical but are now blurred with the outer limits of the GII.

The Canadian military has been involved in OOTW from the earliest days, in securing the Canadian West in 1870 by their useful presence.[22] In 1874, the massacre of the Assiniboine Indians in Western Canada incited Sir John A. Macdonald to form a 300-man paramilitary cavalry force. This force, then known as the North West Mounted Police, was dispatched to assert the Canadian Sovereignty in the West, becoming in fact, members of the first ever Canadian peace-keeping operation.[23]

The CF have a proud history and has demonstrated its professionalism through its numerous involvements in wars, Aid to the Civil Power, and international peacekeeping missions. In the 1994 White Paper, it is stressed that Canada will continue to have a vital interest in doing its part to ensure global security, in the context that its economic future depends on free trade. Although the CF have been constrained in the recent past by fiscal realities, it will continue to offer multi-purpose combat-capable forces for the Defence of Canada and the Canadian sovereignty, for Aid to the Civil Power, and for international peace and security through UN and NATO multilateral operations. Canada has been contributing elements of the CF to numerous UN, NATO and national operations since their inceptions. As the UN is seen as essential for global harmony and progress, and as NATO is seen as a valuable mechanism from preventing the re-nationalisation of defence, Canada's foreign and defence policies will continue to support their operations.[24]

---

[22] Department of National Defence, B-GL-300-000/FP-000 *Canada's Army* (Ottawa: DND Canada, 1998), p 11.

[23] Ibid, p 12.

[24] Ibid, pp 58-59.

The NATO Alliance refers to OOTW as Military Operations Other Than War (MOOTW).[25] As outlined in the NATO doctrine and more specifically in MC 327,[26] MOOTW consists of conflict prevention, arms control and counter proliferation activities, peace support operations, peace building, humanitarian aid operations, and non-combatant evacuation operations.

The newly developed CF IO doctrine of April 1998 parallels the NATO IO doctrine. Although some of the terminology may vary from time to time, it is essentially the same, involving similar types of operations, and recognising the importance of compatibility and inter-operability. NATO is already using IO during MOOTW and Canada and the CF must follow suite to remain a valuable partner. A failure to commit resources to IO may force NATO partners to leverage against the Canadian position for compliance. The North Atlantic Council (NAC) approved MC 402 in August 1997, the NATO Psychological Operations Policy.[27] The Alliance is now engaged in IO, offensively and defensively. IO will normally apply to all five phases of a deployment: preparation and deployment; entry; implementation; transition to peace; and exit.

In the past few years, the CF have downsized, re-organised and re-equipped. The CF are now on their way to becoming smaller, combat-capable, flexible, and affordable,[28] hence

---

[25] MOOTW: A wide range of activities where military capabilities are used for purposes other than large scale combat operations usually associated with war.
NATO, AJP-1 (A), Joint Doctrine, Military Operations Other Than War (MOOTW), ch 23, p 1.

[26] MC 327: NATO Military Planning For Peace Support Operations.

[27] NATO, MC 402, Final Decision (Signed by LGen G.J. Folmer), Psychological Operations Policy, Sep 16, 1997.

[28] World Wide Web. Nahlah, Ayed, "First Military Report Tabled in Parliament", The Evening Telegram, [http://www.southam.com/stjohnseveningtele…newsonw/cpfs/national/981008/n100858.html], October 9, 1998.

capable of meeting their White Paper mandate. Therefore, the CF can accomplish all of their intended missions utilising personnel and equipment designed for much more than OOTW, being capable of directing military force against an adversary. In OOTW, such military capabilities may not be required or may not be welcome in a particular AO. There are several criteria which may limit the use of force or infringe on the current CF capabilities in OOTW: political trends, religious beliefs, country's infrastructure, forces at hand, situation, threats, Rules of Engagement (ROE), and the environment. The AO in which the CF may be asked to participate may require the involvement of many other armed forces, local agencies, national and international organisations, and NGOs.

**Multi-Dimensional OOTW**

Since the end of the Cold War, the nature of the conflicts has gone through significant changes, from international to regional/internal conflicts. The operations conducted under OOTW have similarly changed following the shift in the nature of the conflicts. In a conceptual framework presented by Dr. Eyre from the Lester B. Pearson Canadian International Peacekeeping Training Centre, he described that the classical peacekeeping operations have shifted from being uni-dimensional to being multi-dimensional. He selected four elements of peacekeeping operations to demonstrate the latter point: spectrum, discipline, organisation and media. Operations have gone from a narrow spectrum to a broad spectrum of conflict; the operations conducted in Cyprus under UNFICYP were less involved than those recently conducted in Bosnia under UNPROFOR/IFOR/SFOR. The operations in the Congo (ONUC) involve a large number of militaries but no other parties/belligerents as such when compared against to the operations in the former Yugoslavia which involved many factions. The UN

used to be the only organisation represented in a particular AO; recent events in Somalia, Rwanda, and Haiti demonstrate that a multitude of organisations can now be involved in the same AO. Finally, the media coverage of the US Marines walking on the beach of Somalia upon their arrival would clearly indicate that the media coverage has moved from being a minor issue to being a major one. This shift from uni-dimensional to multi-dimensional has also changed the way militaries conduct OOTW.

In Bosnia-Herzegovina, the NATO Implementation Force (IFOR) AO involved a 36-nation military coalition, five major organisations (NATO, OHR, UNHCR, OSCE, UNMIBH), and several hundred other organisations.[29] Although such a group of organisations may represent a co-ordination challenge, it also represents an infinite amount of information and intelligence, involving IO resources from the entire GII. Some of this information, and more specifically intelligence, might be critical to the conduct of an operation. For example, information gathering from civilian organisations may yield important intelligence information related to the planning of PSYOP[30] campaign or provide the assessment of the effectiveness of such an operation. Close co-ordination with these various organisations is required as it may offer several advantages to the forces involved, inherently contributing to the accomplishment and the success of the mission at hand. Therefore, in the co-ordination of efforts required to accomplish the mission, a Canadian commander may have to utilise a wider range of methods and resources than that normally

[29] Pascale Combelles-Siegel, *Target Bosnia: Integrating Information Activities in Peace Operations* (US: DU Press, 1998), p 115.

[30] PSYOPs are defined as actions to convey selected information and indicators to foreign audiences. They are designed to influence emotions, motives, reasoning, and ultimately, the behaviour of foreign Governments, organisations, groups, and individuals.
Department of National Defence, B-GG-005-004/AF-033 *CF Information Operations* (Ottawa: DND Canada, 1998), ch 2, p 4.

required or available to the CF. This wider range may include IO methods and resources, possibly provided by a member of a

**C2-Protect and C2-Attack**

Data corruption, degradation and destruction of INFOSYS may have negative impacts on the conduct of a mission. All INFOSYS in support of operations, whether in a distant AO or in Canada, will have to be protected. The information technology has yielded the ability to collect, process, and disseminate massive quantities of information/intelligence and in turn, has created a dependency among modern societies and militaries. So much depends on information technology and INFOSYS that this dependency now has the potential to become a centre of gravity.

Adversary forces, political movements and terrorists may utilise PSYOP, deception, electronic warfare, computer network attack, and physical destruction to hamper assigned missions. Information and INFOSYS must be controlled and protected as it affects national and international security. Hence, this will require C2-Protect to be exercised in its full capacity. As all personnel and INFOSYS might be adversely affected, this may also necessitate the employment of the entire spectrum of activities under C2-Attack. All personnel must be information conscious at all times while in an AO; hence, IO training prior to deployment on an OOTW will become a pre-requisite. Therefore, IO must also be incorporated in the educational programmes and the professional development of all DND and CF personnel.

Even though IO activities, such as deception[31] or PSYOP, may not be acceptable to the Alliance, members of the Alliance or local political entities, there remains a requirement

[31] Deception distracts enemy commanders and creates uncertainty in their minds, inducing incorrect conclusions and decisions and out pacing their ability to make decisions.

for the CF to engage in C2-Protect and C2-Attack activities.[32] This will assure the protection of DND/CF personnel and equipment, and will facilitate mission accomplishment.

**PA/PI – PSYOP – CA/CMIC**

This paper will now examine a specific theatre of operations and show the relevance of selected IO components, both offensive and defensive. The discussion will concentrate on three components of IO that will be relevant to the conduct of future OOTW: public information (PI)[33], PSYOP, and CMIC.

Following the signing of the Dayton Peace Agreement and the end of hostilities in the Bosnia-Herzegovina in December 1995, the UN mandated NATO to oversee and enforce a durable cease-fire in that AO. Under the pressure of a perceived failure of the UNPROFOR mission, NATO realised that the future of peacekeeping operations and the credibility of collective security depended on a well-orchestrated public information campaign.[34]
In preparation for IFOR and SFOR, a public information campaign aimed at delivering timely and effective information within the commander's intent was developed. Their concept of operations concentrated on establishing credibility, with both the media and the public. The operations were based on a pro-active public information policy, a free and open media access

---

Department of National Defence, B-GL-300-001/FP-000 *Conduct of Land Operations - Operational Level Doctrine for the Canadian Army* (Ottawa: DND Canada, 1998), ch 7, p 7.

[32] Pascale Combelles-Siegel, *Target Bosnia: Integrating Information Activities in Peace Operations* (US: DU Press, 1998), p 74.

[33] Public Information (PI) is a subset of Public Affairs (PA). PA activities expedite the flow of accurate and timely information to internal (own organisation) and external audiences (the public) audiences.
Department of National Defence, B-GG-005-004/AF-033 *CF Information Operations* (Ottawa: DND Canada, 1998), ch 2, p 6.

[34] Pascale Combelles-Siegel, *Target Bosnia: Integrating Information Activities in Peace Operations* (US: DU Press, 1998), p 5.

policy, and complete, accurate and timely reporting.[35] Although the PI campaign did not start prior to the deployment, perhaps due to time constraints, this pro-active policy was critical early in the operation. It sent a clear message to the factions that the IFOR troops were well-led, well-trained, well-equipped and ready to respond to any challenge through the use of force if necessary.[36]

The PI campaign success was attributed to a functional chain of communication, close relationship between the PI officer and the Commander, and the delegation of release of authority. However, the UK, France and the US had different public information principles drawn primarily from their respective doctrine and Government policies. As an example, different views on the amount of information that could be given to the media could have had potential implications to the success of the allied campaign.[37]

The above statements provide insightful guidance for future Canadian participation in OOTW and for the development of its IO capabilities. A well co-ordinated PI campaign can effectively shape the operational environment, deter potential conflicts, and resolve crisis.[38] By releasing factual information, a well-organised PI campaign can also counter adversary deception and PSYOP.[39] This should encourage the CF to reinforce its CF IO doctrine,

---

[35] Ibid, p 41.

[36] Ibid, p 41.

[37] Ibid, pp 62-63.

[38] Ibid, p 35.

[39] Department of National Defence, B-GG-005-004/AF-033 *CF Information Operations* (Ottawa: DND Canada, 1998), ch 3, p 8.

develop their capability, and acquire the necessary resources for the conduct of PA/PI during OOTW. It also stresses the importance of a strong co-ordination, not only between the Canadian Government and the CF toward the CF IO doctrine, but also toward the Alliance IO doctrine.

The PSYOP campaign was targeted at the local population in the AO. Renamed the IFOR information campaign to detract from a psychological element, it was designed to shape the attitudes and behaviour of the local population in favour of the IFOR/SFOR troops and operations.[40] The bulk of the PSYOP organisation was led by the US and incorporated some supporting elements from France, Germany, and the UK. The PSYOP campaign had limited success.[41]

This situation did not set a very good precedence for future employment of PSYOP during OOTW missions. However, it does provide an incentive for the CF and the Canadian Government to develop PSYOP policies, and to abide by them. It also re-enforces the fact that IO is not exclusive to the military and should involve all of the organisations involved in an AO, including the NGOs. It is interesting to note that the CF do not possess a formal

---

[40] Pascale Combelles-Siegel, *Target Bosnia: Integrating Information Activities in Peace Operations* (US: NDU Press), p 67.

[41] The following is a list of factors that impacted on the campaign:
- reluctance toward PSYOP among NATO partners;
- the C2 situation (can not place US PSYOP forces under NATO C2);
- approval process through a dual chain of command;
- relations with the multinational divisions;
- a weak PSYOP campaign;
- difficult adaptation to the cultural environment;
- relations with International Organisations and NGOs; and
- the difficulty in assessing PSYOP effectiveness.

Ibid, pp 82-104.

PSYOP capability, but that the CF IO doctrine insists that PSYOP must be considered for the effective integration of all IO capabilities.[42] If the latter is true, then the CF must develop some PSYOP capabilities for without it, the CF IO doctrine will loose some of its credibility. Since Canada has already agreed to MC 402 in September 1997, this paper offers that the role of the CF in up-coming OOTW missions will decrease considerably, should a policy decision other than supporting a PSYOP capability is taken. The national responsibilities[43] would indicate that it is not a matter whether Canada should be debating the policy, but a matter of how many CF resources should be directed toward a CF PSYOP capability.

A third element of IO employed during IFOR/SFOR was CMIC. These activities were aimed at publicising the mission accomplishments of several military units within the AO. Unfortunately, good news does not sell newspapers, and the CMIC activities did not arouse media interests.[44] This is deplorable in the context that these activities could have enhanced US troop morale in particular, but were instead curtailed by a leadership oversight.[45] Better examples of CMIC are available from OOTW in which the CF participated. The media

---

[42] Department of National Defence, B-GG-005-004/AF-033 *CF Information Operations* (Ottawa: DND Canada, 1998), ch 2, p 3.

[43] Specific national responsibilities are:
- considering PSYOP during the planning process and implement it into directives;
- to develop plans and programs in support of NATO PSYOP policy and doctrine;
- to ensure that, within their capabilities and overall priorities, intelligence and research and analysis is provided in support of NATO PSYOP;
- to ensure interoperability is taken into consideration during development and procurement of PSYOP capabilities;
- to include PSYOP in education, training and exercises as appropriate; and
- to provide resources and trained personnel to support NATO PSYOP in operations and exercises.

NATO, MC 402, Final Decision (Signed by LGen G.J. Folmer), Psychological Operations Policy, Sep 16, 1997, p 5.

[44] Pascale Combelles-Siegel, *Target Bosnia: Integrating Information Activities in Peace Operations* (US: NDU Press, 1998), p 114.

[45] Ibid, p 111.

releases related to the OKA crisis, Somalia, the Red River flooding, and the recent Ice Storm operations are examples of successful CIMIC operations. As a critical element of IO, the CF must remain engaged in all aspects of CA/CIMIC activities.

Under the concepts of IO, CIMIC operations may also integrate other functions such as PI and PSYOP. The full integration of PI, PSYOP and CMIC were seen as crucial in the Bosnia-Herzegovina AO, with the aim of co-ordinating and synchronising the messages so they reinforce each other.[46] Furthermore, internal and external co-ordination operated as force multipliers for the NATO commanders in Bosnia.[47] For example, proper internal co-ordination allowed the IFOR commander to combine PI and PSYOP and effectively reach various audiences. This re-affirms that IO will be paramount to the success of future OOTW.

In the context of multi-dimensional OOTW, and in reviewing particular elements of IO, such as inter-operability, C2-Protect, C2-Attack, PI, PSYOP and CMIC, it can be concluded that the CF must develop their capabilities across the full spectrum of IO activities, both offensive and defensive. This would ensure that they meet their scope of maintaining peace, defusing crisis, and deterring conflict during OOTW missions. Even though the employment of offensive IO capabilities during OOTW may require Cabinet approval,[48] the CF must

---

[46] Ibid, p 174.

[47] Ibid, p 142.

[48]Department of National Defence, B-GG-005-004/AF-033 *CF Information Operations* (Ottawa: DND Canada, 1998), ch 2, p 8.

refocus their strategy, policies and acquisition programmes toward the full integration of IO capabilities and resources.

It must be noted at this juncture, that the 1999 Defence Planning Guidance (DPG) states in part that: "…it is important for DND and the CF to proceed apace with efforts to translate these emerging concepts into operational capabilities, in particular to adequately protect our own operational C2 systems."[49] However, the following guidance is also provided: " The DCDS and the Defence CIO [Chief Information Officer] have been tasked to jointly develop, seek DMC approval and implement policy and doctrine for IO within the DND/CF in conjunction with OGDs and other Canadian agencies as well as our Allies. Priority is to be given to the development of a defensive IO capability."[50] The addition of the statement related to defensive operations represents a shift of focus from the 1998 Defence Planning Guidance. However, it can not be interpreted as a total departure from the existing requirement of an offensive capability. As stated in the CF IO doctrine: "IO requires the close integration of offensive and defensive capabilities and activities …"[51]

While Canada may not be able to afford all IO capabilities and its related resources, Canada must, as a minimum, acquire those that are directly related to national OOTW operations and those that are identified by the CF as mandatory for future UN or NATO lead

[49] World Wide Web. Department of National Defence, Canada, "*Defence Planning Guidance 1999",* [http://131.137.255.5/vcds/dgsp/dpg/dpg99/chap1_e.asp], May 15th, 1999, p 4.

[50] Ibid, p 4.

[51] Department of National Defence, B-GG-005-004/AF-033 *CF Information Operations* (Ottawa: DND Canada, 1998), ch 1, p 7.

OOTW. The development of niche capabilities would offer certain advantages and should be further explored.

**Structures**

The CF will not be able to achieve these goals in isolation. It is already recognised that the tools or weapons to conduct information warfare exist at the present time and could affect everyone and everything in the GII, hence the NII and the DII. As these weapons pose a threat to the national security, there is a requirement to protect all combatants and non-combatants.[52] This can be achieved with a structure that will concentrate and co-ordinate the efforts of the civil, military, Government, and industrial sectors of the nation.[53]

The 1997 Defence Planning Guidance contained the following directive: "to translate emerging concepts into operational capabilities [to protect Canada's operational command and control systems]."[54] Concurrently, the 1997 Defence Planning Guidance also directed the DCDS to develop an IO strategy for DND and the CF, and to organise, equip and train for IO. An IO Steering Committee (IOSC) was formed to develop IO policy and doctrine, and to guide the IO Working Group (IOWG) and the CF IO developments.

---

[52] World Wide Web. Colonel Richard Szafranski, "A Theory of Information Warfare. Preparing for 2020", USAF, [http://www.uta.fi/ptmakul/infowar/lw2.html], p 1.

[53] Colonel Alward, Information Operations Briefing to CFIPC, May 1998, p 7.

[54] Colonel Joseph Stevens, "Information Operations in DND/CF", *Canadian Government Executive*, 1998, Vol. 3, No.2, p 10.

The SCIOG and the IOWG have made excellent progress in restructuring and guiding the CF toward future IO involvement. On April 1st 1998, the CF established the Canadian Forces Information Operations Group (CFIOG), under the Defence Information Services Organisation (DISO), also known as the Defence Chief Information Officer (CIO). DISO is organisationally located under the VCDS. Figure 1 outlines the CFIOG organisation.

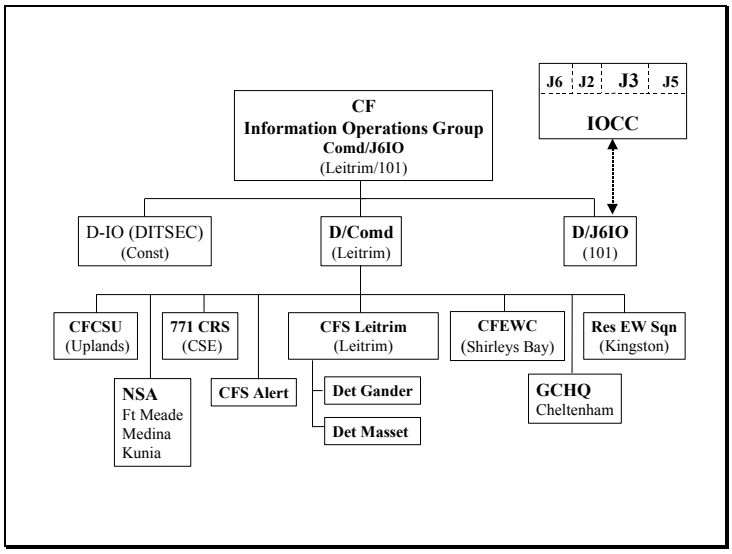


**Figure 1**

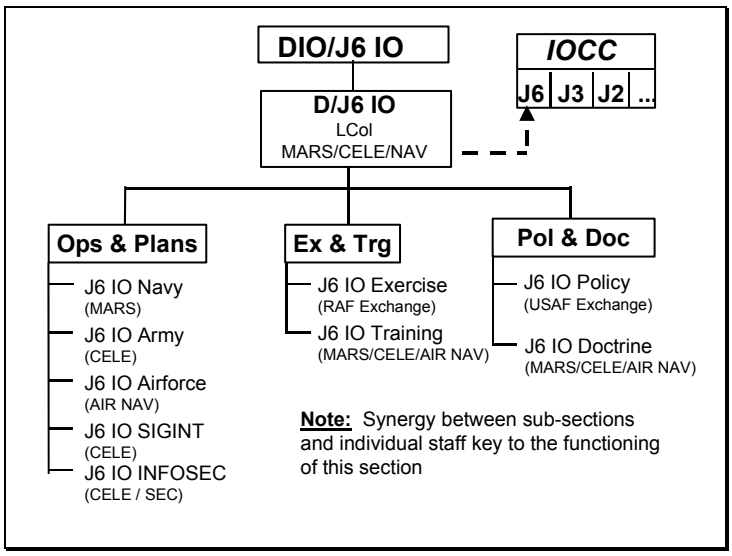

**Figure 2**

The key element in the CFIOG organisation will be the Information Operations co-ordinating Cell (IOCC). The IOCC has been created in accordance with the CFIO doctrine[55] and will ensure that IO becomes an integral part of all military operations, including OOTW, at both the national and operational levels. Figure 2 depicts a typical IOCC and its footprint on the CF. The IOCC structure also allows IO connectivity with Other Government Departments (OGDs), through the DND/CF organisational structures. The SCIOG and the IOWG are making every effort possible to raise the awareness of a co-ordinated IO strategy in Canada, and as such, are involving OGDs and other agencies: DFAIT, Transport Canada, Industry Canada, RCMP, CSIS, and CSE. In an international context, they are also working with the US, the UK, and NATO. As well, they already have MOUs in place with the US Joint Command and Control Warfare Centre, and the UK Air Warfare Centre.[56]

Although the current CFIOG structure will eventually integrate all elements and components of the DND/CF organisations as applicable to IO, it is not clear on how this interface will be achieved with every other Government departments, civilian, and industrial organisations in Canada. As all of these organisations may have an impact on the conduct of future OOTW, there are obviously key national issues to be resolved. The Government of Canada will have to become fully involved, perhaps through the Privy Council Office, if IO

[55] Department of National Defence, B-GG-005-004/AF-033 *CF Information Operations* (Ottawa: DND Canada, 1998), ch 4, p 1.

[56] Colonel Alward, Information Operations Briefing to CFIPC, May 1998, p 21.

matters that can affect the entire nation are to be co-ordinated.[57] As it stands, it is the contention of this paper that the IOSC, the IOWG and the CFIOG organisations will be the catalysts in raising IO awareness in Canada vis-à-vis its potential impact on national security issues.

There is, however, the possibility of an even stronger catalyst: Operation ABACUS. As the year 2000 approaches, there are a number of uncertainties as to how the millennium bug will affect the entire INFOSYS and all of the services for which they were designed. Operation ABACUS is the CF response to these potential problems and their effect on the national security. The Joint Task Force (JTF) was assigned to conduct the operational level planning.[58] One of the constraints in the planning guidance is that the CF will depend on Government, agencies and industries as well as the national infrastructure to execute its tasks and responsibilities.[59] One of the JTF implied tasks is to identify operational and tactical level CIMIC requirements, structure, and training.[60] Finally, one of the Commander's criteria for success is the maintenance of a pro-active, successful Public Affairs plan throughout the operation.[61]

---

[57] Ibid, pp 24-26.

[58] The JTF has been given the following mission: " On order, the JTF will provide assistance, throughout Canada, to the civil authorities, in order to maintain services and infrastructure affected by the year 2000 Problem that are essential to life and public order."
Colonel T.J. Calvin, Joint Task Force Headquarters (JTFHQ) COS Planning Directive 001 Op ABACUS, 3120-10(J7 Coord), October 1998, p 2.

[59] Ibid, p 3.

[60] Ibid, p 3.

[61] Ibid, p 5.

Clearly, Operation ABACUS will involve IO and the new CFIOG structure. Operation ABACUS should raise the awareness of every Canadian toward the importance of protecting information and the INFOSYS. The CF will have to develop close working relationships with every OGDs, all Governments, industries, and NGOs. The PA campaign will have to be designed to provide timely and effective information in order for the CF and the Canadian Government to maintain a high degree of credibility. These functions will have to be co-ordinated under the IOCC and their success will demonstrate that the IO doctrine is sound and supported, and that the new structure is viable. The success of Operation ABACUS may be crucial to the future of IO in the CF, and to the conduct of OOTW, at home or abroad. The scope of activities required to protect the information environment in Canada will most likely be very expensive.[62] This will require a very strong political support, both moral and financial, across all Government departments and the nation at large.

**Political Support**

Canada has long recognised the importance of information and intelligence, and as such, has been involved in security operations since 1864.[63] In 1946, the Communications Branch of the National Research Council (CBNRC) was created with the responsibility for providing SIGINT to meet the needs of the federal Government. In 1947, it also took on the

---

[62] World Wide Web. Graeme Browning. "Infowar", The Daily Fed, National Journal, [http://www.govexec.com/dailyfed/0497/042297b1.html], April 21, 1997.

[63] In 1864, Sir John A. Macdonald for the purpose of watching and patrolling the whole frontier from Toronto to Sarnia created The Western Frontier Constabulary, a detective and preventive police force. Another force, the Montreal Water Police, a federal agency as well, looked after Eastern Canada. It also reported to Macdonald. These forces operated along the upper Canada borders and rail lines, reporting on activities related first to the American Civil War, then to Fenians whose goal was to overthrow English rule in Ireland.
World Wide Web. "A Historical Perspective on CSIS", [http://www.csis-scrs.qc.ca/eng/backgrnd/back5e.html], 1996.

responsibility of serving as the Canadian Government's communications-electronic security (COMSEC). In 1975, CBNRC was transferred to DND and renamed the Canadian Security Establishment (CSE). The Canadian Forces Supplementary Radio System (SRS) collects SIGINT and operates under CSE. Both organisations work in close relationships with the NSA in the US, the Government Communications Headquarters (GCHQ) in the UK, the Defence Signals Directorate (DSD) in Australia, the Government Communications Security Bureau in New Zealand and a number of other SIGINT agencies around the world. The Minister of National Defence is responsible for CSE issues in Cabinet and in Parliament. The Privy Council Office exercises policy and operational control of CSE while the Deputy Minister of National Defence exercises administrative control of CSE.[64]

CSIS and its RCMP antecedence effectively dates back to 1864 and again shows the seriousness of the Government to deal with intelligence and security issues. CSIS is responsible to the Solicitor General of Canada. In 1992, CSIS was formally tasked to review the changing security intelligence environment to determine if the service should restructure and what resources would be necessary to respond to the changing environment. It was found that the service was well structured to respond to the changing security intelligence environment. A report was tabled in the House of Commons in 1992 and CCIS has been releasing an annual report ever since.[65] In the context of IO, the 1997 report addresses the

[64] World Wide Web. Bill Robinson, [brobinso@watserv1.uwaterloo.ca], "The Communications Security Establishment: An Unofficial Look Inside Canada's Signals Intelligence Agency", [http://watserv1.uwaterloo.ca/-brobinso/cse.html#FAC], 1998, p 5.

[65] The report is aimed at keeping the public informed about the service and its responsibilities for public safety and national security, hence providing a powerful tool for the CSIS organisation, but also for the Government officials who have to stay abreast of matters that could affect the life or well-being of their constituents.
World Wide Web. "Canada Security Intelligence Service", [hhtp://www.csis-scrs-qc.ca/eng/publicrp/pub1997e.html#7], 1997, p 1.

global security environment; it is interesting to note that out of ten public safety and national security points of interests, six are directly related to IO.[66] It is even more interesting to note that out of fifteen identified counter-terrorism threats, eleven are directly to IO.[67] Under an Information Warfare heading, the reports warns of the threats posed to computer-based systems: "CSIS co-operates with several Government departments to counter the threat from information operations, and provides assessments on Canadian vulnerabilities and the capabilities of those who might exploit them."[68]

---

[66] Out of 10 security areas, the following pertains to IO:
- as a country with freedoms that others can exploit relatively easily, Canada is interested in curtailing the activities against Canada of foreign intelligence services;
- as a member of the G7 and a leading industrial country, Canada is interested in protecting Canadian Government and business information from intrusion by foreign Governments;
- as a country with highly-rated quality of life, Canada is interested in a reduction of transnational criminal activities which have a damaging effect on society;
- as a country dependent upon intelligence-sharing responsibilities with allies, Canada in interested in promoting cooperation with other intelligence services
- as country with a large immigration program, Canada is interested in protecting immigrants from harassment, intimidation and coercion by outside influences; and
- as a country with a relatively small population in a relatively large landmass, Canada is interested in the effectiveness of the collective security organisations to which it belongs.

Ibid, p 3.

[67] Counter-terrorism: once established in Canada, terrorist groups tend to follow a familiar pattern of behaviour, which may include any or all of the following activities:
- raising funds openly or covertly in support of terrorist activities;
- engaging in illegal activities to raise money;
- attempting to influence public or political opinions in Canada;
- recruiting new members and supporters;
- conducting offensive and defensive intelligence surveillance;
- aiding the entry of terrorists in Canada by legal or illegal means;
- making fraudulent use of false or valid travel documentation;
- arranging the illegal transit of members to the US and other countries;
- countering rival organisations in Canada;
- influencing or intimidating members of their own expatriate community; and
- planning and participating in domestic and foreign terrorist operations.

Ibid, p 3.

[68] Ibid, p 7.

IO, whether conducted by friend or foe, have no delineated front lines. Attacks of computerised train control systems in Japan and the release on the Internet of British secure installation drawings from a remote location,[69] should serve as examples that Canada is more vulnerable to terrorism attacks than in the past. As Canada is becoming more dependent on information technology, it provides an adversary with a target rich and readily accessible environment. Systems such as transportation, pipe lines, electricity, communications, financial institutions, and a multitude of secure and non-secure databases are IO targets. Keeping in mind that technological developments are available to both friend and foe alike, countering the threats to the INFOSYS will not be an easy task.[70] The argument is further fuelled with the following quote from Winn Schwartau, a communication specialist: " … government and commercial computer systems are so poorly protected today that they can be essentially considered defenceless."[71]

The Canadian Government must realise that OOTW as conducted in the past did not pose direct or immediate threats to national security. As civilians and soldiers are now intertwined,[72] it is important that their respective systems be protected so as not to interfere with one another. Future missions may draw unpopularity in a given AO and may yield repercussions for the homeland INFOSYS. Conversely, frictions at home could reach the

---

[69] World Wide Web. Mathiew G. Devost , Brian K. Houghton, Neal A. Pollard, "Information Terrorism: Can you thrust your toaster?", [http://www.ndu.edu/ndu/inss/siws/ch3.html], 1998, p 3.

[70] Lieutenant Commander Harley from the US Navy wrote: "… there is always the danger that technology gaps will close, sometimes suddenly. Advances breed either duplication by the enemy or effective counters." World Wide Web. Lieutenant Commander Jeffrey A. Harley, "Information, Technology, and the Centre of Gravity", US Navy, [http://www.usnwc.edu/nwc/art4wi97.htm], 1997, p 4.

[71] Alvin Toffler and Heidi Toffler, *War and anti-war: survival at the dawn of the twenty-first century* (Canada: Little, Brown and Company (Canada) Limited, 1993), p 149.

[72] Ibid, p 152.

soldiers in a distant AO. Dedicated resources such as CFIOG, CSE and CSIS are essential to OOTW and the national security; they must also co-ordinate their efforts in their fight to ensure the protection of all information and all INFOSYS in Canada.

By supporting CFIOG, CSE, and CSIS, the Canadian Government has demonstrated its understanding of the potential impacts that information and intelligence threats may have on the national security. The CSIS report is clear and in protecting its national security, the Canadian Government will have to support, both morally and financially, the internal activities related to IO.

Recently, the Canadian Government has again showed its political support by directing the CDS toward a national OOTW in support of the federal government response to the potential effects of the millennium bug, Operation ABACUS. This operation aims at minimising the negative effects posed by the Year 2000 problem. However, the political support provided thus far might be interpreted as being only moral support as the CF may be called upon to assist the civil authorities in every way possible but within the resources available.[73] I believe that the millennium bug is only the first problem that we encounter that may affect the entire nation.[74] At the Armed Forces Communications and Electronics Association (AFCEA) breakfast in May 1998, the Honourable Art Eggleton, Minister of

---

[73] Operation ABACUS, COP 01, October 1998, p 1.

[74] Government departments have already spent more that $400 M to replace some of their INFOSYS, and they did not have a choice.
World Wide Web. Valerie Lawton , "Ottawa Takes Swat at the Millennium Bug ", The Toronto Star, [http://www.thestar.com/back_issues/ED19981006/news/981006NEW06_NA-BUG6.html], 6 October 1998, p 2.

National Defence, offered reassuring words: " But, as on other fields, in other days, we will respond to these threats to our freedoms and do whatever is necessary to combat them."[75]

Given the Canadian Government's long history of supporting intelligence requirements in order to protect the national security, the Government will have no other choice but to provide moral and financial support for the development of the CF IO capabilities, and possibly in the near future, for the co-ordination and integration of all information/intelligence agencies under one national organisation. The Canadian Government must also encourage initiatives in the arena of information technologies; these initiatives should be aimed at identifying potential causes of and responses to information attacks.

**Conclusion**

The evolution of technology and the integration of INFOSYS into the spectrum of war-fighting operations have created the requirement for a new tool of warfare, Information Operations. The CF IO doctrine under an OOTW perspective is all encompassing and blends well with the NATO doctrine. If developed, it will allow the CF to operate effectively in any OOTW, at home or abroad. The doctrine recognises the importance of inter-operability vis-à-vis the multiplicity of militaries, agencies, and organisations that may be present in a particular AO. It also recognises the importance of education and training. The CF IO doctrine must be understood by the military, but also by the Canadian Government. Moreover, it is unlikely that

[75] The Honorable Art Eggleton, Speech to the Armed Forces Communications and Electronics Association (AFCEA) Breakfast, May 28, 1998, p 3.

the CF will be able to afford the critical components of their IO doctrine if it is not effectively funded, and if IO is not readily recognised as a mandatory and integrated component of future OOTW.

Components of IO, more particularly PI, PSYOP and CIMIC have been relatively successful in the Bosnia-Herzegovina AO. The fact is that IO is already in use under NATO operations (PI, PSYOP, and CIMIC) and that Canada must move forward promptly, in conjunction with its military partners. As well, since Canada has already agreed to MC 402, the CF must seek a clear policy on PSYOP as it may limit the use of CF elements in a UN or NATO-led OOTW.

If the CF aspire to meet its scope of maintaining peace, defusing crisis and deterring conflict during OOTW, they must be allowed to develop their IO capabilities. As a minimum, Canada must fund the IO activities that are directly related to national OOTW and those that are identified by the CF as mandatory for future participation in UN or NATO lead OOTW. The development of niche capabilities would offer certain advantages and should be looked at closely. Therefore, the CF may not be able to participate in future OOTW without a properly developed IO capability and dedicated resources.

The CF have created a new structure (CFIOG) under the VCDS, which should be capable of handling the co-ordination of IO across all military operations. The IOCC is a key element of the CFIOG organisation as it offers co-ordination within the department, and with the various OGDS, agencies, and NGOs. Operation ABACUS is coming at an opportune

time. It should provide a clear indication as to whether or not the CFIOG meets its intended goals, but more importantly, ABACUS may heighten the awareness of IO at the national level. It is concluded that the new structure is sufficient to assure the conduct of IO by the decision makers in future OOTW.

Canada has always recognised the importance of information/intelligence and its potential impact on national security. In that light, Canada must continue to support the CF IO doctrine, CFIOG, CSE, and CSIS as well as encouraging IO initiatives and the national co-ordination of IO activities. There might also be a future requirement to integrate all existing IO organisational resources. It is concluded that Canada must provide the required financial, moral, and political support for the development of an IO capability for use by the CF in OOTW.

**Recommendations**

It is recommended that:

- the spectrum of IO activities, described under the CF IO doctrine, be developed for CF future involvement in OOTW, including PSYOP;
- the Canadian Government provides its full support to the CF IO activities, the acquisition of required resources, and to the CFIOG;
- the Canadian Government must continue to support CSE and CSIS, and encourage their co-ordination with CFIOG;
- the Canadian Government must encourage initiatives in the field of IO; and

- the Canadian Government must task an overall managerial team to ensure that all IO efforts are co-ordinated, ensuring the national objectives are met.

## Annotated List of Works Cited

Ames, Roger T. *The Art of War*. US: Ballantine Books. 1993. Eloquent work describing the writings of Sun Tzu.

Alward, Colonel. Information Operations Briefing to CFIPC. May 1998. A comprehensive briefing given several times by its author. The briefing outlines the emergence of Information Operations and its importance for all Canadians. The briefing then explains how CFIOG was set up and how it is meant to interact with the remainder of the Headquarters, and the principal organisations dealing with intelligence and information in Canada and abroad.

Calvin, T.J., Colonel. Joint Task Force Headquarters (JTFHQ). COS Planning Directive 001, Op ABACUS. 3120-10 (J7 Coord). October 1998. This document addresses them proper steps of an operational planning process as related to Operation ABACUS. Its mission is for JTF to provide assistance, throughout Canada, to the civil authorities in order to maintain services and infrastructure affected by the Year 2000 Problem that are essential to life and public order.

Canada, Department of National Defence. B-GL-300-000/FP-000 *Canada's Army*. Ottawa: DND Canada, 1998. 1-28. This publication describes Canada's Army in all of its aspects. It provides an excellent history of the Canadian Army, and its contribution to building and defending the nation.

Canada, Department of National Defence. B-GG-005-004/AF-033 *CF Information Operations.* Ottawa: DND Canada, 1998. This publication represents the Canadian Forces doctrine on Information Operations. It is generally well-written and uses terminology, which is compatible with the NATO and US doctrines.

Canada, Department of National Defence. B-GL-300-001/FP-000 *Conduct of Land Operations - Operational Level Doctrine for the Canadian Army*. Ottawa: DND Canada, 1998. This document describes the operational doctrine adopted by the Canadian Army. Chapter 7 is dedicated to Information Operations.

Canada, Department of National Defence. 1994 Defence White Paper. Ottawa: DND Canada, 1994. This document identifies the mandate of the Canadian Forces and the type of forces Canada requires. The aim is for Canada to have a multi-purpose combat capable force.

Canada, Department of National Defence. Operation ABACUS COP 01, 3120-10 (J7). October 1998. This draft document describes all possible phases and requirements of Operation ABACUS as they pertain to missions, operations, task allocation, command and signals, infrastructures, training, etc…

Collin, John ,Lieutenant-Colonel. Chief Joint Plans Section, Information Operations Planning Briefing, 1998. This briefing outlines the use of Information Operations in future conflicts.

Combelles-Siegel, Pascale. *Target Bosnia: Integrating Information Activities in Peace Operations*. US: DU Press, 1998. This book presents an excellent review of IFOR and SFOR operations in Bosnia-Herzegovina as they relate to Information Operations. The major points of discussion center around are the Public Affairs campaign, more specifically Public Information, Civil-Military relations and Psychological Operations. Several examples are provided and each section provides lessons learned and recommendations for future operations.

Eggleton, Art, The Honorable. Speech to the Armed Forces Communications and Electronics Association (AFCEA) Breakfast. May 28, 1998. This speech addresses the threats posed to the security of information and electronically stored data. It recognises the importance of Information Operations, briefly describes the new CFIOG organisation and the establishment of Network Vulnerability Assessment Team and a Computer Emergency Response Team.

NATO. AJP-1 (A) *Joint Doctrine*. This document represents NATO's Joint doctrine for all operations.

NATO. MC 402. Final Decision (Signed by LGen G.J. Folmer). *Psychological Operations Policy*. September 16, 1997. This official document outlines the Psychological Operations Policy adopted by NATO. It contains a list of definitions and outlines the responsibilities of the Military Committee, Major NATO Commanders, and Nations.

Stevens, Joseph, Colonel. "Information Operations in DND/CF." *Canadian Government Executive*, Vol. 3, 1998, pp 10-11. This short article explains the importance of Information

Operations in Canada. It also discusses the extent of the problems associated with electronic information and Command and Control Warfare in action.

Toffler, Alvin and Toffler, Heidi Toffler. *War and anti-war: survival at the dawn of the twenty-first century*. Canada: Little, Brown and Company (Canada) Limited, 1993: 149-173. This section of the book gives examples of info-terror, fragility of INFOSYS, and tools to conduct information warfare. The author also makes the point that the civilian INFOSYS are inter-connected or intertwined with the military and that information protection is very much relevant.

US, Department of the Army. FM 100-6. *Information Operations Doctrine*. Washington, DC: Government Printing Office, 1996. This publication outlines the Army doctrine as it relates to Information Operations. It provides an excellent baseline on Information Warfare and a very good framework to analyse other doctrines in the field of Information Operations.

World Wide Web. Ayed, Nahlah. " First Military Report Tabled in Parliament." The Evening Telegram.[http://www.southam.com/stjohnseveningtele…newsonw/cpfs/national /981008/n100858.html]. October 9, 1998. This article looks at the first report made in Parliament on the state of the Canadian Military. It addresses downsizing problems, quality of life issues and that the CF are on their way to becoming smaller, combat-capable, flexible, affordable and good to personnel.

World Wide Web. Browning, Graeme. "Infowar." The Daily Fed. National Journal. [http://www.govexec.com/dailyfed/0497/042297b1.html], April 21, 1997. This article looks into the near future and identifies that the threat posed to INFOSYS is real and already here. The article discusses attacks against INFOSYS that have already taken place and identifies the requirements for centers at the National Security Agency and the Defense INFOSYS Agency.

World Wide Web. Canada. Department of National Defence. *Defence Planning Guidance 1999*. [http://131.137.255.5/vcds/dgsp/dpg/dpg99/chap1_e.asp]. May 15, 1998. The Defence Planning Guidance 1999 provides a framework for translating Government direction as established in the Defence White Paper into a capable and efficient Defence Services Program that delivers affordable multi-purpose, combat capable armed forces for Canada. The document is applicable for Fiscal Years 1999-2000 through 2003-2004 and beyond.

World Wide Web. Devost Mathiew G., Houghton Brian K., Pollard Neal A. "Information Terrorism: Can you thrust your toaster?" [http://www.ndu.edu/ndu/inss/siws/ch3.html]. 1998. This paper discusses information terrorism as related to Information Warfare, and identifies tools and possible targets. Lastly, it proposes an integrated structure that would combine the investigative and jurisdictional assets of law enforcement with the offensive capabilities of the military.

World Wide Web. Harley, Jeffrey A., Lieutenant Commander. "Information, Technology, and the Centre of Gravity." US Navy. [http://www.usnwc.edu/nwc/art4wi97.htm]. 1997. This paper discusses information and technology as tools of warfare, but also the risks associated

with these two fields. The discussion leads to the point where information technologies have become a centre of gravity; he uses Warden's five ring model to demonstrate as an example, that leadership, or command and control is always the centre of gravity. Finally, he recommends that centre of gravity decision models are useful analytical tools and should be discussed further.

World Wide Web. Lawton, Valerie. "Ottawa Takes Swat at the Millennium Bug." The Toronto Star. [http://www.thestar.com/back_issues/ED19981006/news/981006NEW06_NA-BUG6.html]. October 6, 1998. Article describing the problems associated with Year 2000 and outlining that the RCMP have already cancel leave from December 27th, 1999 until March 15th, 2000. The article expands on readiness programmes and safety issues.

World Wide Web. "Canada Security Intelligence Service." [http://www.csis-scrs.qc.ca/eng/publicrp/pub1997e.html#7]. 1997. This is the 1997 CSIS public report. The report discusses in some details the global security environment, counter-terrorism, and counter-intelligence. It also discusses Information Warfare, proliferation of weapons of mass destruction, and transnational criminal activity.

World Wide Web. "A Historical Perspective on CSIS." [http://www.csis-scrs.qc.ca/eng/backgrnd/back5e.html]. 1996. This article provides the historical background of CSIS, its reason d'être and their evolution in the domain of intelligence. It also introduces the reader to creation of the 1992 first public report.

World Wide Web. Robinson, Bill. [brobinso@watserv1.uwaterloo.ca]. "The Communications Security Establishment: An Unofficial Look Inside Canada's Signals Intelligence Agency." [http://watserv1.uwaterloo.ca/-brobinso/cse.html#FAC]. 1998. An interesting paper on the Canadian Security Establishment (CSE). It provides an overview and a brief historical perspective, discusses CSE budgets, personnel manning, and policy, operational and administrative control. The paper concludes that an oversight mechanism is required for CSE.

World Wide Web. Szafranski, Richard, Colonel. "A Theory of Information Warfare. Preparing for 2020." USAF. [http://www.uta.fi/ptmakul/infowar/lw2.html]. This paper discusses the tools of Information Warfare and the importance to protect both combatants and non-combatants against them. It also discusses the fragility of knowledge and beliefs, potential target sets, and the complexity of Information Warfare.

World Wide Web. US, Russia's Nuclear Force Sinks With the Rubble, Economic Crisis Erodes Strategic Arsenal, The Washington Post, [http://www.washingtonpost.com/wp-srv/Wpcap/1998-09/18/055r-091898-idx.html], September 18, 1998. Recent article discussing problems affecting the Russian nuclear arsenal and its detection system. The article discusses the displeasure of Russian missile commanders, the weaknesses of their detection systems vis-à-vis the Russian nuclear safety programme.